REMARKS

The examiner withdrew the objection to the drawings.

35 U.S.C. §102

The examiner rejected Claims 8, 9,11-13,15,16, and 18-21 under 35 U.S.C. 102(e) as being anticipated by US Patent Publication 2004/0010718 to Porras et al.

Claim 8, as amended, includes the features of "... retrieving a baseline list of port protocols used by a host ... the baseline list listing service and/or port protocols used by that host over a baseline period that is of a longer duration that a current period, retrieving a current list of service and/or port protocols currently being used by the host ... determining whether there is a difference ... and if there is a difference, indicating a new service ... ."

The examiner argues that:

> **As per claim 8, Porras et al discloses a method for detection of a new service involving an entity, the method comprises: Porras et al discloses monitoring network activity of an entity (see page 1, paragraph 11) that meets the recitation of entity being tracked, which includes analyzing event records such as port protocols (see page 3, paragraph 31) the method includes collecting statistical measures that includes port protocols over a period of time comprising the most recent data represented as short-term statistical profiles (current list) and the normal, non recent, data as long-term statistical profiles (baseline list) (see page 1, paragraphs 11 and 15, page 3, paragraphs 33 and 36 and page 4, paragraph 40) that meets the recitation of retrieving a baseline list of port protocols used by a entity being tracked, the baseline value determined over a baseline period, retrieving a current list of port protocols for the entity being tracked; and further discloses a comparison is made between the two wherein the difference between them indicates suspicious network activity or abnormal activity (see page 1, paragraphs 11 and 15) or indication of new service (see page 3, paragraphs 33 and 36 and page 4, paragraph 47) that meets the recitation of determining whether there is a difference in the port protocols, by having a protocol that was in a current list but was not in the baseline list; and if there is a difference; indicating a new service involving the tracked entity. (emphasis omitted)**

Essentially, the examiner argues that the alleged teachings: "**the method includes collecting statistical measures that includes port protocols over a period of time comprising the most recent data represented as short-term statistical profiles (current list) and the normal, non recent, data as long-term statistical profiles (baseline list)**" correspond to the baseline and current lists of claim 8.

Porras however discloses that: "**[0034] A monitor 16 can also construct interval summary event records, which contain accumulated network traffic statistics (e.g., number of packets and number of kilobytes transferred).**" Porras does not disclose that this statistical information is somehow used to construct the claimed baseline and current lists. Porras also discloses that:

> **[0047] Signature analysis can also scan traffic directed at unused ports (i.e., ports to which the administrator has not assigned a network service). Here, packet parsing can be used to study network traffic after some threshold volume of traffic, directed at an unused port, has been exceeded. A signature engine 24 can also employ a knowledge base of known telltale packets that are indicative of well-known network-service protocol traffic (e.g., FTP, Telnet, SMTP, HTTP). The signature engine 24 then determines whether the unknown port traffic matches any known packet sets. Such comparisons could lead to the discovery of network services that have been installed without an administrator's knowledge.**

Thus, rather than retrieving a baseline list of protocols used by a host ... over a baseline period and retrieving a current list of service and/or port protocols currently being used by for the host, Porras teaches to study those ports that the administrator has not assigned a network service to (missing therefore unassigned services to assigned ports). In this technique there does not exist the baseline list or the current list, but rather just unassigned ports that the signature analysis monitors.

While Porras discloses a technique that determines unknown port traffic, Porras would use that finding to compare to know packet sets, not a current list of ports being used by the host or to the baseline list of ports.

Therefore, to the extent that Porras discloses a new service detection technique, it is fundamentally different than that claimed by Applicant.

<u>Claim 9</u>

Claim 9 depends directly from claim 8, and requires: "determining if the entity is providing or using the new service." The examiner uses paragraph 33, 36 and 47 which are reproduced above to reject claim 9 without specifically pointing out relevant discussions in these paragraphs. However, as understood, these passages neither describe nor suggest: "determining if the entity is providing or using the new service." Applicant's claim 9 is distinct and allowable over the art.

In addressing Applicant's prior reply the examiner argues that: "**Regarding claim 9, Porras discloses in paragraph 47, the new service has been installed by the entity, and network service using ports that are not authorized by an administrator, which meets the claimed limitation.**" With all due respect the mere fact that Porras discloses "**network services that have been installed without the knowledge of the administrator,**" says nothing about whether the host is using or providing the installed service. Therefore, claim 9 further distinguishes over Porras.

Claims 10-14 are allowable for at least for the reasons discussed in claim 8.

Claim 15 and dependent claims 16-22 drawn to a computer program product analogue of claims 8-14, are allowable for analogous reasons as those given for claim 1 and the respective dependent claims.

<u>35 U.S.C §103</u>

The examiner rejected Claims 10, 14, 17, and 22 under 35 U.S.C. 103(a) as being unpatentable over Porras et al.

The Examiner argues that:

> **As per claim 10, Porras et al substantially discloses determining whether the activity exceeds a threshold value when the entity is using a new service (unknown port) and if the threshold exceeds and the entity is using a new service, anomaly is detected (see page 4, paragraphs 47 and 48). Porras et al suggests using a countermeasure response to report the anomaly (see pages 6-7, paragraphs 67 and 71). Although not using the same terms as the claim language it is apparent to one of ordinary skill in the art of intrusion detection that a rule for issuing an alert may be defined as exceeding a threshold value which indicates an attack as disclosed Porras et al and producing a countermeasure response or reporting the attack in response to detecting can be reasonably interpreted as generating an alert. As known in the art, in an attack-response method when an attack is detected according to a specified rule, an alert is generated. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to issue an alert if is determined whether a rule specifies to issue an alert if the entity is providing or using the new service; and if it is also determined that the entity is providing or using the new service so as to protect the network from more global attacks by taking further actions (see page 7, paragraph 68) or by alerting other entities (see page 2, paragraph 16) as suggested by Porras et al..**

Porras in 0047 and 0048 teaches to apply signature analysis to scan traffic directed at unused ports (i.e., ports to which the administrator has not assigned a network service to). Porras neither describe nor suggest "determining if the host is providing or using the new service." Rather, Porras applies a threshold value of traffic to a specific port to detect and report suspicious activities, but does not differentiate if the host is providing or using the new service before issuing an alert as required by claim 10. Applicant's claim 19 is distinct and allowable over Porras. Claim 17 recites similar features in claim 10 and therefore allowable at least for the reasons given in claim 10.

In rejecting claim 14, the Examiner acknowledges in the Office Action on page 6 that:

> **"As per claim 14, Porras et al substantially discloses measuring network connections and using a statistical profile to make the comparison (see page 1, paragraph 1-2) but does not explicitly disclose that the statistical profile is represented as a connection table. Examiner takes official notice that it is very well known in the art that network events can be represented in a form of a table and it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the statistical profile of measures of network connections of Stewart et al and implement it in a connection table so as to make it easier for reading, editing, and interpreting the data as known in the art. (emphasis added)"**

The examiner acknowledges that Porras does not teach the claimed connection table. Applicant had requested that the Examiner provide documentary evidence to support the statement[1] that: "**it is very well known in the art that network events can be represented in a form of a table and it would have been obvious to one of ordinary skill in the art at the time the invention was made... .**" The examiner replied as:

> **With respect to claim 14, Examiner has provided applicant with prior art references for representing network events in a table. See, for instance, US 2003/0145225 to Bruton, 111 et al fig. 17 and paragraph 45. See US Patent 5,999,179 to Kekic, fig. 3 and US Patent 7,047,288 to Cooper et al. With regard to claim 1, Cooper discloses a field that depicts a range to track an entity by specifying for instance the policy domains, time domain or the monitoring points (see fig. 3, 5, IOC, fig. 21, and 31). Therefore, upon further consideration, applicant has not overcome the rejection of claim 1. In view of the above the claims remain rejected.**

Neither Bruton nor Kekic nor Cooper suggests the claimed connection table.[2] Moreover, the examiner in the above statement has not properly apprised the examiner of where in Kekic or Cooper this feature is allegedly taught.

[1] MPEP 2144.03 states that "if applicant challenges a factual assertion as not properly officially noticed or not properly based upon common knowledge, the examiner must support the finding with adequate evidence ... If applicant adequately traverses the examiner's assertion of official notice, the examiner must provide documentary evidence in the next office action if the rejection is to be maintained.

[2] Bruton does not suggest the claimed feature in Fig. 17, which depicts a table that shows "Policy Sensitivity and Event Suspicion Levels for TCP Port Scan."

Kekic does not suggest the claimed feature in Fig. 3 (which is not findable in Kekic) or any of the other figures.

Accordingly Applicant renews this request and requests that the examiner furnish proof of a "**connection table**" in the context of Applicant's claimed invention.

Applicant also requests that the examiner clarify the reference to "Stewart et al.," because Applicant is unable to identify any reference with that name.

The examiner rejected Claims 1-7 under 35 U.S.C. 103(a) as being unpatentable over Porras et al in view of US 7,047,288 (Cooper et al.)

Claim 1 calls for "A graphical user interface for configuring a new service detection process...comprising: a first field that depicts choices for entities to track in the network; a second field that allows a system to track if the selected entity is providing or consuming a service; a third field that depicts a range over which to track an entity selected in the first field; and a fourth field to specify a severity for an alert generated if a new service is detected."

The Examiner argues that:

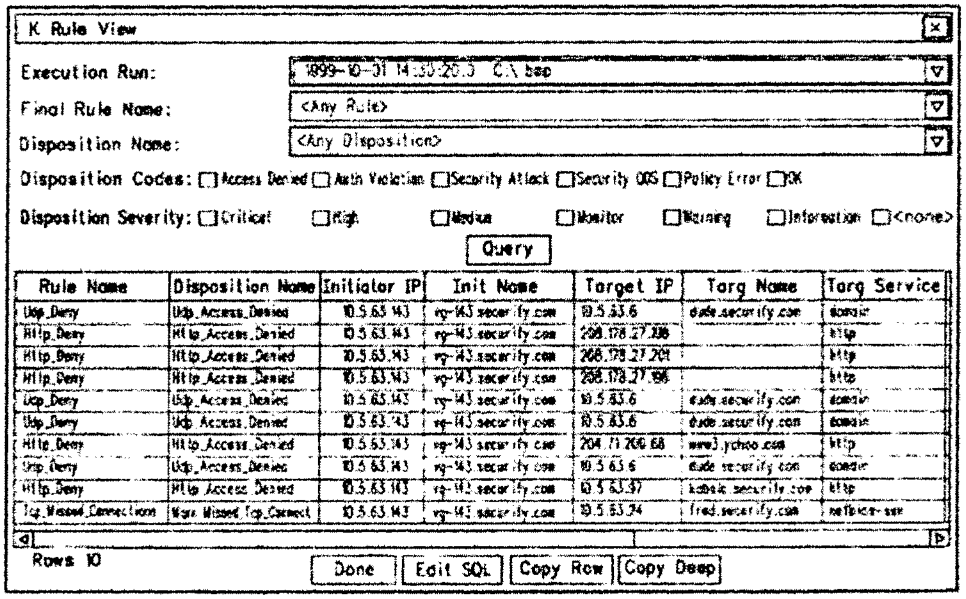
> **As per claim 1, Porras et al substantially discloses a graphical user interface (see page 3, paragraph 31) for configuring a new service detection process, and discloses tracking an entity in the network (see page 1, paragraph 11) a method that allows a system to track if the selected entity is providing or consuming a service (such as using unknown port protocol) (see pages 4-5, paragraphs 40-41, 47-48); depicts a range over which to track the selected entity (see page 3, paragraph 35); specifying severity for an alert generated if a new service is detected (see pages 4-5, paragraphs 41, and 47-48; and pages 6-7, paragraph 67). Porras et al does not explicitly disclose the details of the graphical user interface. However, it would have only required routine skill in the art to implement the step above into fields in a graphical user interface to make it interactive. Cooper et al in an analogous art teaches generating a human readable English language description of a formal specification of network security policy that allows non-technical user within a user's organization to comprehend the policy by making the description simple enough to understood (see abstract). Cooper et al discloses a graphical user interface (see for instance fig. 9) that includes several fields including field for specifying a host name, field for service being tracked (see figs. 9 and 31) that meets the recitation of a first field that depicts choices for entities to track in the network, field for specifying a range of the entity being tracked (see column 13, lines 25-67 and fig. 9) and field specifying a severity for an alert generated (see fig. 9). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was make to modify Porras et al to implement the method disclosed by Porras et al into a graphical user interface represented by fields as disclosed in Cooper et al. One of ordinary skill in the art would have been recognized the advantages disclosed by Cooper et al who teaches generating a human readable English language description of a formal specification of network security policy that allows non-technical user within a user's organization to comprehend the policy by making the description simple enough to understood (see abstract).**

Cooper does not suggest the claimed feature. While Cooper discusses "A common connection structure 6109 allows connection data to be arranged in a stack allocation for each access across layer boundaries." referencing figure 17, that feature does not correspond to the claimed connection table.

Porras however mentions a graphical user interface at 0081. Nothing in 0081 or elsewhere in Porras discloses a graphical user interface for configuring a new service detection process. Rather, as the examiner readily acknowledges Porras does not disclose any of the details of the graphical user interface.

The examiner inexplicitly relies on Cooper to teach all the elements of claim 1 even though Cooper does not teach for configuring a new service detection process.

However, Fig. 9 (reproduced below) in Cooper shows a queried rule view dialog box. In particular, it shows that the null.spw policy has denied all traffic (col. 12 lines 1-8). However, Fig. 9 and its corresponding descriptions in Cooper do not describe "a third field that depicts a range over which to track an entity selected in the first field." The selections of "Final Rule Name" and "Disposition Name" from respective pull down menus in Fig. 9 merely offer the user the policy rules that can be applied and policy of what action or state change needs to take place in response to a network event (see col. Table A terminologies of Rule and Disposition).



Execution Run: 1999-10-31 14:35:20.3 C:\ bsp

Final Rule Name: <Any Rule>

Disposition Name: <Any Disposition>

Disposition Codes: □Access Denied □Auth Violation □Security Attack □Security DOS □Policy Error □OK

Disposition Severity: □Critical □High □Medium □Monitor □Warning □Information □<none>

Rule Name	Disposition Name	Initiator IP	Init Name	Target IP	Targ Name	Targ Service
Udp_Deny	Udp_Access_Denied	10.5.63.143	vq-143.security.com	10.5.63.6	dade.security.com	domain
Http_Deny	Http_Access_Denied	10.5.63.143	vq-143.security.com	208.178.27.206		http
Http_Deny	Http_Access_Denied	10.5.63.143	vq-143.security.com	208.178.27.201		http
Http_Deny	Http_Access_Denied	10.5.63.143	vq-143.security.com	208.178.27.196		http
Udp_Deny	Udp_Access_Denied	10.5.63.143	vq-143.security.com	10.5.63.6	dade.security.com	domain
Udp_Deny	Udp_Access_Denied	10.5.63.143	vq-143.security.com	10.5.63.6	dade.security.com	domain
Http_Deny	Http_Access_Denied	10.5.63.143	vq-143.security.com	204.71.200.68	www3.yahoo.com	http
Udp_Deny	Udp_Access_Denied	10.5.63.143	vq-143.security.com	10.5.63.6	dade.security.com	domain
Http_Deny	Http_Access_Denied	10.5.63.143	vq-143.security.com	10.5.63.37	kabala.security.com	http
Tcp_Missed_Connections	Warn_Missed_Tcp_Connect	10.5.63.143	vq-143.security.com	10.5.63.34	fred.security.com	netbios-ssn

Rows 10

FIG. 9

The Examiner also argues that the discussion at col. 13 lines 25-67 discloses that "a third field that depicts a range over which to track an entity selected in the first field." Applicant disagrees. In contrast, this portion of discussion refers to Fig. 11 which shows a high-level view of an example network. However, that discussion does not concern a graphical user interface for configuring a new service detection process (see reproduced Fig. 11 below), and the discussion is silent with regard to "a third field that depicts a range over which to track an entity selected in the first field."

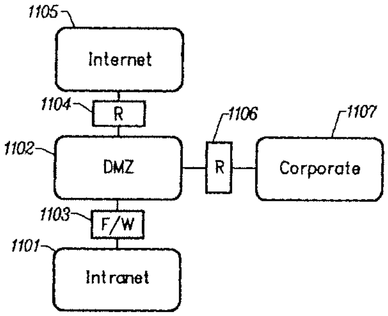


FIG. 11

Accordingly, because Porras does not teach features of the graphical user interface and Cooper likewise does not teach these features, the combination of Porras and Cooper cannot teach the features of Applicant's claim 1 and therefore claim 1 is distinct and allowable over Porras in view of Cooper.

Claims 2-7 are allowable at least for the reasons discussed in claim 1.

All of the dependent claims are patentable for at least the reasons for which the claims on which they depend are patentable.

Any circumstance in which the applicants have (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

In view of the foregoing, applicants respectfully request entry of the amendment since it addresses specific objections first raised by the examiner in the instant office action, does not require any further consideration or search. Accordingly, applicants submit that the application is in condition for allowance and such action is respectfully requested at the examiner's earliest convenience.

Please apply any other charges or credits to deposit account 06-1050.

No fee is due. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 9/23/08

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (877) 769-7945